Министерство образования и науки Российской Федерации

(МИНОБРНАУКИ РОССИИ)

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (ТГУ)

Институт прикладной математики и компьютерных наук

Кафедра защиты информации и криптографии

**КУРСОВАЯ РАБОТА**

БИБЛИОТЕКА ДЛЯ РАБОТЫ С БУЛЕВЫМИ ФУНКЦИЯМИ ДЛЯ ЯЗЫКА ПРОГРАММИРОВАНИЯ LYAPAS

Муругов Михаил Алексеевич

Руководитель

канд. физ.-мат. наук, доцент

\_\_\_\_\_\_\_\_\_\_\_\_И.А.Панкратова «\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_201\_\_\_г.

Студент группы № 1155

\_\_\_\_\_\_\_\_\_\_\_\_\_М.А.Муругов

Томск 2018

ОГЛАВЛЕНИЕ

Введение………………………………………………………………………………………….2

1. Описание алгоритмов на математическом языке
   1. Принадлежность булевой функции к классу 
   2. Принадлежность булевой функции к классу 
   3. Преобразование Мёбиуса булевой функции
   4. Принадлежность булевой функции к классу линейных булевых функций
   5. Принадлежность булевой функции к классу самодвойственных булевых функций
   6. Отражение вектора значений булевой функции
2. Программные реализации
   1. Принадлежность булевой функции к классу 
   2. Принадлежность булевой функции к классу 
   3. Преобразование Мёбиуса булевой функции
   4. Принадлежность булевой функции к классу линейных булевых функций
   5. Принадлежность булевой функции к классу самодвойственных булевых функций
   6. Отражение вектора значений булевой функции
   7. **///Нужно ли включать реализации, не описанные в 1.x?///**
3. Экспериментальные данные
4. Заключение

Список использованных источников и литературы

Приложения

**ВВЕДЕНИЕ**

Целью этой курсовой работы было написание библиотеки для работы с булевыми функциями для языка программирования LYaPAS. В дальнейшем планируется, что эта библиотека будет использоваться для реализации криптографических алгоритмов и прочих нужд.

**///Нужно ли как-то переделать введение?///**

**ОПИСАНИЕ АЛГОРИТМОВ НА МАТЕМАТИЧЕСКОМ ЯЗЫКЕ**

***Принадлежность булевой функции к классу ***

**Определение.** Булева функция *сохраняет константу 0* (*принадлежит классу* *)*, если на наборе из всех нулей функция принимает значение нуль.

Алгоритм:

Вход:  – булева функция

Выход: “ принадлежит классу ?”

Шаг 1) Если , то ответ “Да”

Иначе ответ “Нет”

***Принадлежность булевой функции к классу ***

**Определение.** Булева функция *сохраняет константу 1* (*принадлежит классу* ), если на наборе из всех единиц функция принимает значение единица.

Алгоритм:

Вход:  – булева функция

Выход: “ принадлежит классу ?”

Шаг 1) Если , то ответ “Да”

Иначе ответ “Нет”

***Преобразование Мёбиуса булевой функции***

**Определение.** *Положительной конъюнкцией* называется элементарная конъюнкция, не содержащая инверсий переменных. Договоримся обозначать положительную конъюнкцию через .

**///Определение АНФ взять из “Булевы функции в криптографии”! (не нашёл)**

**Определение.** *Полиномом Жегалкина*, или *алгебраической нормальной формой (АНФ)*, булевой функции  называется дизъюнкция с исключением различных положительных конъюнкций переменных из множества , то есть формула вида , задающая функцию .

**Определение.** Преобразованием Мёбиуса называется функция , где  – множество всех булевых функций от переменных. С помощью преобразования Мёбиуса решается задача построения АНФ булевой функции, и вычислить его значения для функции  можно по формуле . Рассмотрим возможный способ выполнения этого вычисления.

**///Убрать способ? Написать сразу рекурсивный алгоритм? Как должна выглядеть в тексте ссылка на литературу? Надо ли приводить подытоживание(краткую суть способа)?///**

Построим матрицу отношения предшествования булевых векторов , строкам и столбцам которой сопоставлены булевы векторы длины и

Например, ;

Нетрудно убедиться, что и , где – вектор-столбец значений функции . Если и — соответственно младшая и старшая половины вектора значений , то по формуле получим следующую рекурсивную формулу:

.

На «дне» рекурсии для функции от одной переменной

На основании этого способа преобразование Мёбиуса реализовано программно.

***Принадлежность булевой функции к классу линейных булевых функций***

**Определение.** *Длиной* булева вектора назовем количество его компонент, а *весом* вектора – количество компонент, равных единице

Длину булева вектора  в дальнейшем будем обозначать . Запись , где  – булева функция, будет обозначать длину вектора её значений.

Вес булева вектора  в дальнейшем будем обозначать . Запись , где  – булева функция, будет обозначать вес вектора её значений.

**Определение.** *Длиной полинома Жегалкина назовем* количество конъюнкций в полиноме, а его *степенью* – наибольший из рангов конъюнкций, входящих в полином.

**Определение.** Полином Жегалкина называется *линейным*, если его степень не превышает единицы.

**Определение.** Булева функция называется *линейной* (*принадлежит классу* ), если ее полином Жегалкина линеен.

Алгоритм:

Вход:  – булева функция

Выход: “ – линейна?”

Шаг 1) 

Шаг 2) Если полином Жегалкина, построенный по коэффициентам  линеен, то ответ “Да”

Иначе ответ “Нет”

***Принадлежность булевой функции к классу самодвойственных булевых функций***

**Определение.** Булева функция  называется *двойственной булевой функции* , если она получена из  инверсией всех аргументов и самой функции, то есть .

**Определение.** Булева функция  *самодвойственна* (*принадлежит классу* ), если она равна двойственной себе функции, то есть .

Алгоритм:

Вход:  – булева функция

Выход: “ – самодвойственна?”

Шаг 1) Для всех векторов  таких, что :

Шаг 1.1) Если , то ответ “Нет”

Шаг 2) Ответ “Да”

***Отражение вектора значений булевой функции***

**Определение.** Отражением вектора значений булевой функции является обмен значениями на противоположных наборах аргументов.

В дальнейшем отражение вектора значений булевой функции  будем обозначать 

Алгоритм:

Вход:  – булева функция

Выход: 

Шаг 1) Для всех  таких, что :

Шаг 1.1) 

**ПРОГРАММНЫЕ РЕАЛИЗАЦИИ**

Перед изложением дальнейшего материала необходимо кое-что обозначить:

Во-первых, булевы функции в языке LYaPAS представляются векторами их значений.

Во-вторых, вектора значений булевых функций хранятся в логических комплексах L, каждый элемент которого занимает в памяти 4 байта(32 бита). Таким образом, т.к. , то функция до 5 аргументов включительно помещается в один элемент комплекса. От 6 в 2 элемента, от 7 в 4 и т.д. Количество элементов комплекса, необходимых для хранения функции от  аргументов можно вычислить по формуле .

***Принадлежность к классу ***

Проверка булевой функции на принадлежность к классу  тривиальна. Необходимо просто посмотреть на первый бит вектора её значений. Если этот бит равен нулю, то функция сохраняет константу 0.

***Принадлежность к классу ***

. Для проверки принадлежности булевой функции к классу  необходимо посмотреть на старший бит вектора её значений. Если этот бит равен 1, то функция сохраняет константу 1. Но проверка булевой функции на принадлежность к классу  немного сложнее, чем к классу , т.к. у функций, зависящих от  аргументов старший бит вектора значений находится в нулевом элементе комплекса и его сначала необходимо найти. В общем же случае найти старший бит вектора значений функции можно по следующим правилам: , , где  – индекс элемента комплекса, а  – номер бита в элементе с индексом .

***Преобразование Мёбиуса булевой функции***

Как следует из способа, изложенного в **[ссылка на “БФвК”]**, преобразование Мёбиуса рекурсивно реализуется по следующему алгоритму:

Шаг 1) Разбиваем вектор значений булевой функции на младшую и старшую часть  и  соответственно

Шаг 2) 

Шаг 3) Если , то выход

Иначе выполнить эту процедуру для  и 

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ**

1. Быкова С.В. Учебно-методический комплекс «Булевы функции». Томск 2006.
2. Панкратова И.А. Учебное пособие «Булевы функции в криптографии». Томск 2014.